Definition and validation of a business IT alignment method for enterprise governance improvement in the context of processes based organizations - presentation

Feltus, Christophe

Publication date:
2008

Document Version
Peer reviewed version

2008 Corporate Governance of IT International Conference

Wellington New Zealand
December 1 - 2

Definition and validation of a business IT alignment method for enterprise governance improvement in the context of processes based organizations

Christophe Feltus, Centre de Recherche Public Henri Tudor – LUXEMBOURG
Michaël Petit, Computer Science Department FUNDP – BELGIUM
Georges Ataya, Solvay Business School ULB – BELGIUM

Review of existing

AC Models …

AC model and Responsibility's Concepts

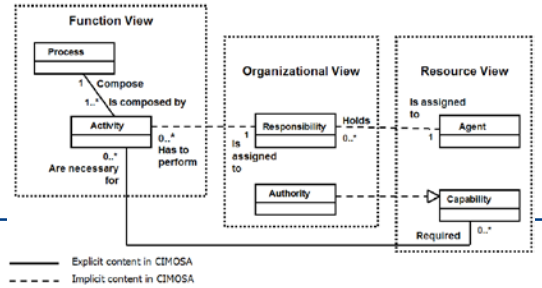
	MAC	DAC	RBAC	UCON
Subject	Yes	Yes	Yes	Yes
Object	Yes	Yes	Yes	Yes
Group	No	User Group	Role	Defined by objects and subject's attributes
Capability	Access Right	Access Right	Access Right	Access Right
Accountability (Obligation, Constraint)	No	No	Yes, static and dynamic separation of duty	Defined by objects and subject's attributes
Commitment	No	No	No	No

RE Models …

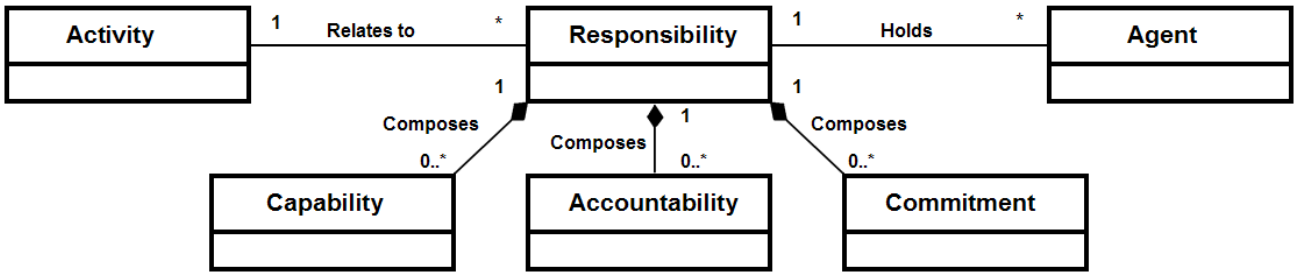
Engineering Methods and Responsibility's Concepts.

	KAOS	I*	GBRAM	ARMF	RACAF	Scenario Driven	Uses Cases
Subject	Agent	Actors	Agent	Users	Actors	Subject	Actors
Object	Yes	Yes	-	Asset	Data	-	Object
Group	-	Yes	-	Yes	Yes	Yes	Yes
Capability (Right, Authorzation)	Authorization rules	Abilities and beliefs	-	Permission	Permission	Permission	Access right
Accountability (Obligation, Constraint)	Achieve requirements and expectations	Goal	Achieve a goal	Perform a task	Perform a task	Perform a scenario	Pre-conditions, post-conditions
Commitment	No	Yes	No	No	No	No	No

EAM Models …



The model…

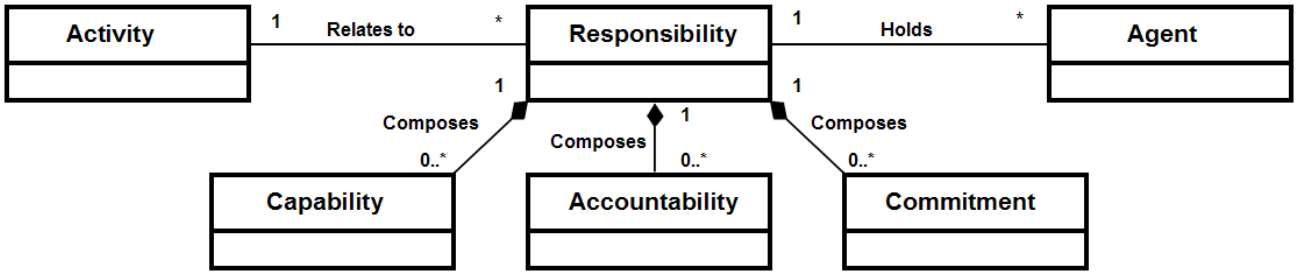


Accountability **: which describes the state of being answerable about the achievement of an activity.**

Commitment **: is the moral engagement of an agent to fulfill an activity and the assurance that he will do it in respect of an ethical code.**

Capability **: which describes the require qualities skills or resources to perform an activity.**

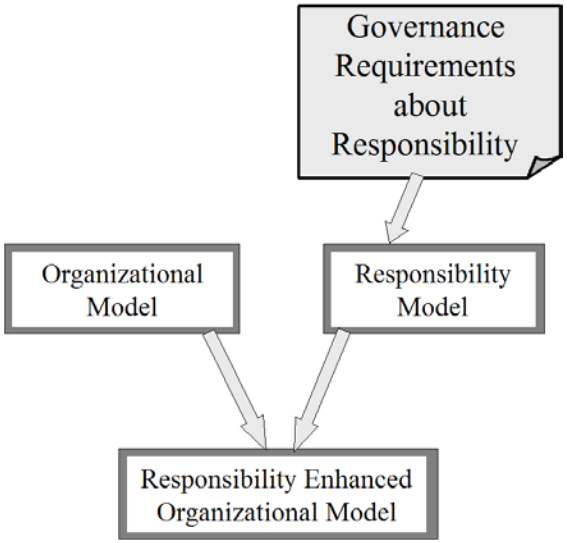
The model…



Advantages

- Responsibility are clearly established and understood
- Accountability is linked to an agent rather to a group of agent (like role)
- It increases the ethic of the business
- It guarantees the right capability of the right agent. Not more, not less.

The model…



Policy elicitation : The model advantage is a strong framework for policy elicitation.
The model may address all level of the organisation
The policies may be technical as well as managerial

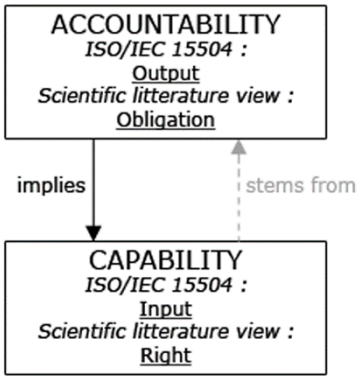
Enhancement of models : Lot of models do not deeply address the responsibility.
We join those models with the responsibility model
The models are closer to governance requirements

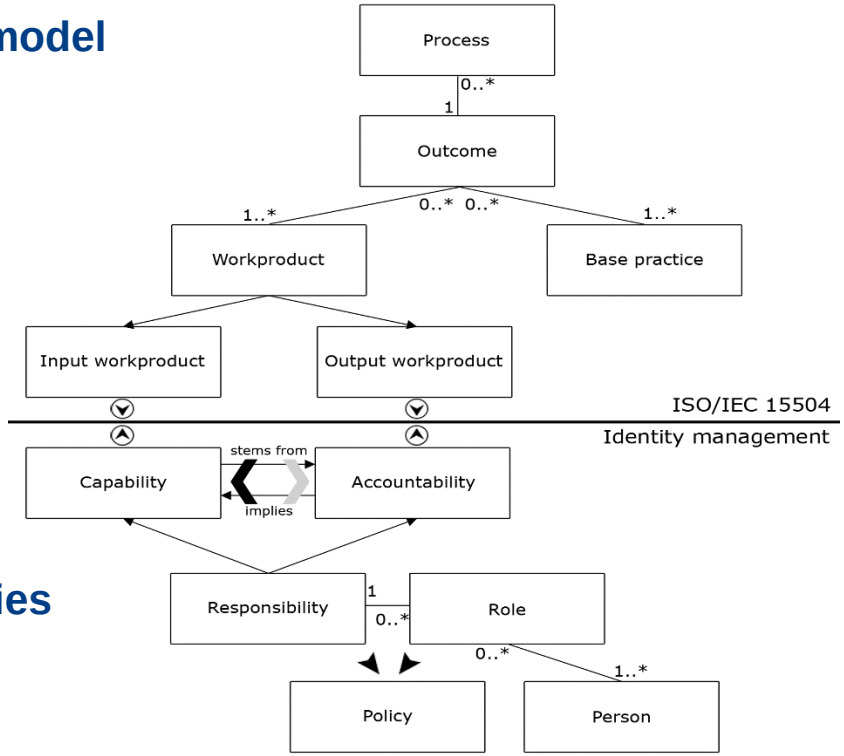
Standard enforcement in practices :
The model provide material to enhance the practice

ISO/IEC 15504

- ISO/IEC 15504 provides a processes structure and a maturity model
- Responsibility is not centric in the standard. It is addressed in Level 2 of the MM
- Basically, the standard may not be used to define policies

→ We make links between the standard and our model



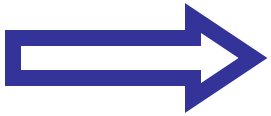


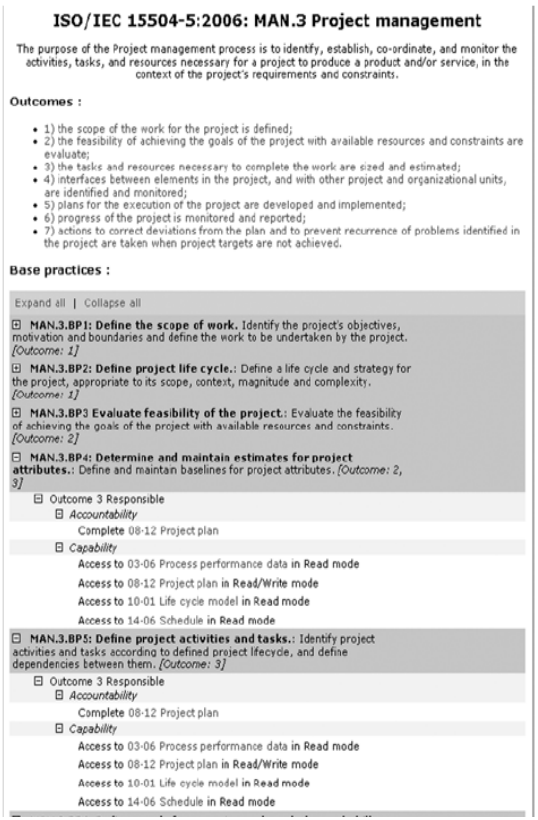
- Based on that link, it is possible to define policies aligned to business requirements

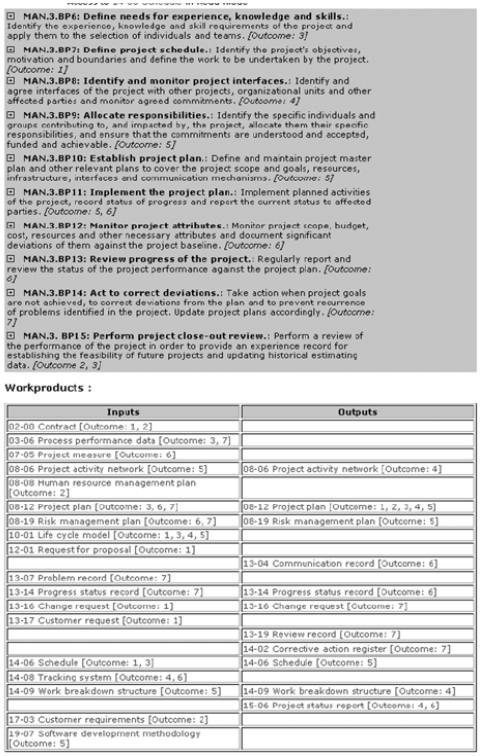
ISO/IEC 15504

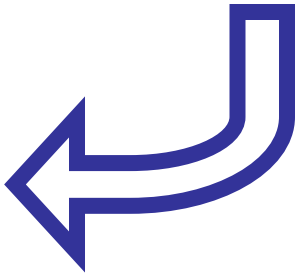
MAIN CONCEPTS OF THE PROJECT MANAGEMENT PROCESS

ISO/IEC 15504-5:2006 → MAN.3 Project management	
Purpose	The purpose of the Project management process is to identify, establish, co-ordinate, and monitor the activities, tasks and resources necessary for a project to produce a product and/or service, in the context of the project's requirements and constraints.
Outcomes	… 3) the tasks and resources necessary to complete the work are sized and estimated; …
Base Practices	… MAN.3.BP4: Determine and maintain estimates for project attributes. Define and maintain baselines for project attributes. [Outcome: 2,3] MAN.3.BP5: Define project activities and tasks. Identify project activities and tasks according to defined project life cycle, and define dependencies between them. [Outcome: 3] …
Workproducts inputs	… 03-06 Process performance data [Outcome: 3,7] 08-12 Project plan [Outcome: 3, 6, 7] 10-01 Life cycle model [Outcome: 1, 3, 4, 5] 14-06 Schedule [Outcome: 1, 3] …
Workproducts output	… 08-12 Project plan [Outcome: 1, 2, 3, 4, 5] 14-06 Schedule [Outcome: 5] …









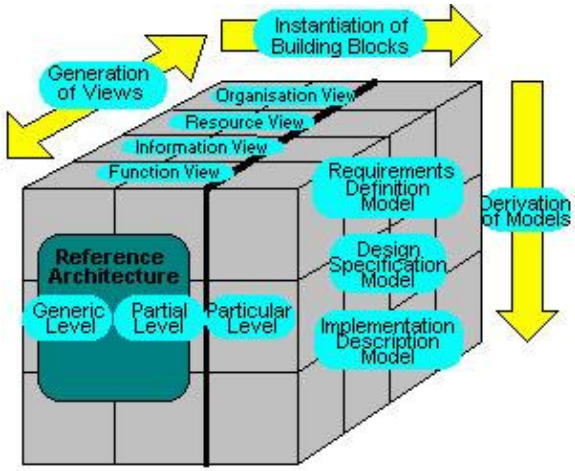
```
<Target>
  <Subjects>
    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        42
      </AttributeValue>
      <SubjectAttributeDesignator AttributeId="contact_id"
        DataType="http://www.w3.org/2001/XMLSchema#string"
        MustBePresent="true"/>
    </SubjectMatch>
  </Subjects>

  <Actions>
    <Action>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
          read
        </AttributeValue>
        <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
          AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
        </ActionMatch>
      </Action>
    </Actions>

  <Resources>
    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        14-06 Schedule
      </AttributeValue>
      <ResourceAttributeDesignator
        AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
        DataType="http://www.w3.org/2001/XMLSchema#string"/>
    </ResourceMatch>
  </Resources>
</Target>
```

CIMOSA EAM

CIMOSA is a modelling framework that provides semantic unification of the concepts from a system architecture.



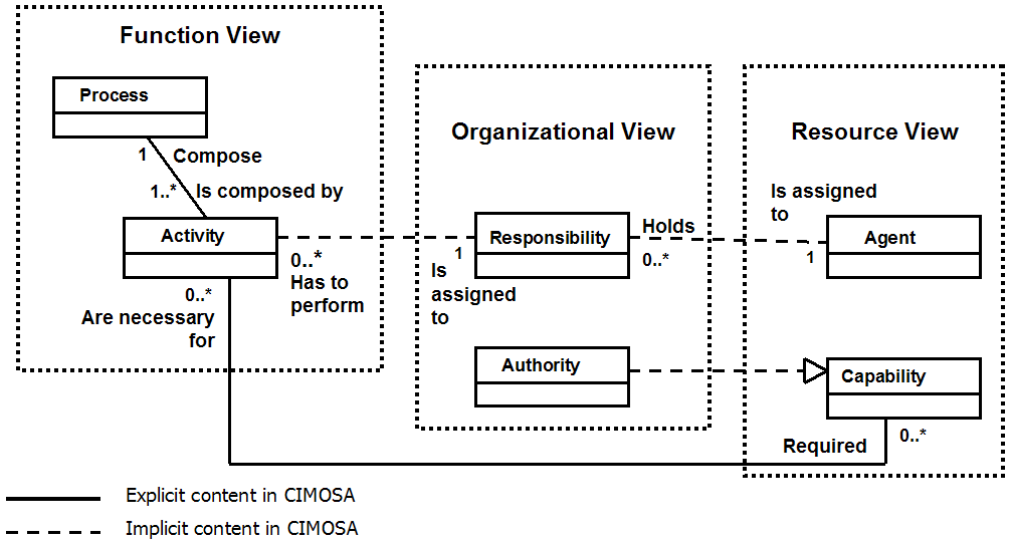
It contains three axes (CIMOSA Cube) :
- **GENERATION (with 4 views : Function, Information, Resources and Organization)**
- **INSTANTATION**
- **DERIVATION**

Agent = functional entity
→represented in resource view

Responsibility
→represented in organization view

Capability
→represented in resource view

No commitment, no link between accountability and responsibility



CIMOSA EAM

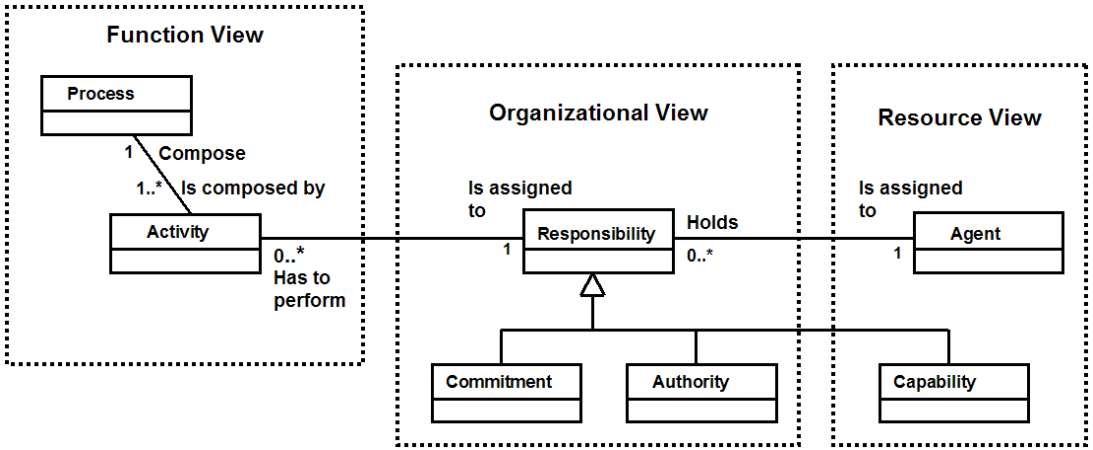
Enhancement :

- Responsibility explicitly introduced in organization view
- Responsibility is linked to an activity and to an agent

- Capability no more linked to the activity but is linked to the responsibility

- Commitment is introduced

- Accountability is formally a component of the responsibility



ResourceInput: *Name of resource*
Responsibility:
Accountable : *list of accountabilities*
Capability : *list of capabilities*
Commitment :*list of commitments*

ISO/IEC 38500:2008

The principle :

2.1.1 Principle 1: Responsibility

Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.

ISO/IEC 38500:2008 requirement (from Principle 2 : Strategy) :

Direct
Directors should direct the preparation and use of plans and policies that ensure the organization does benefit from developments in IT.

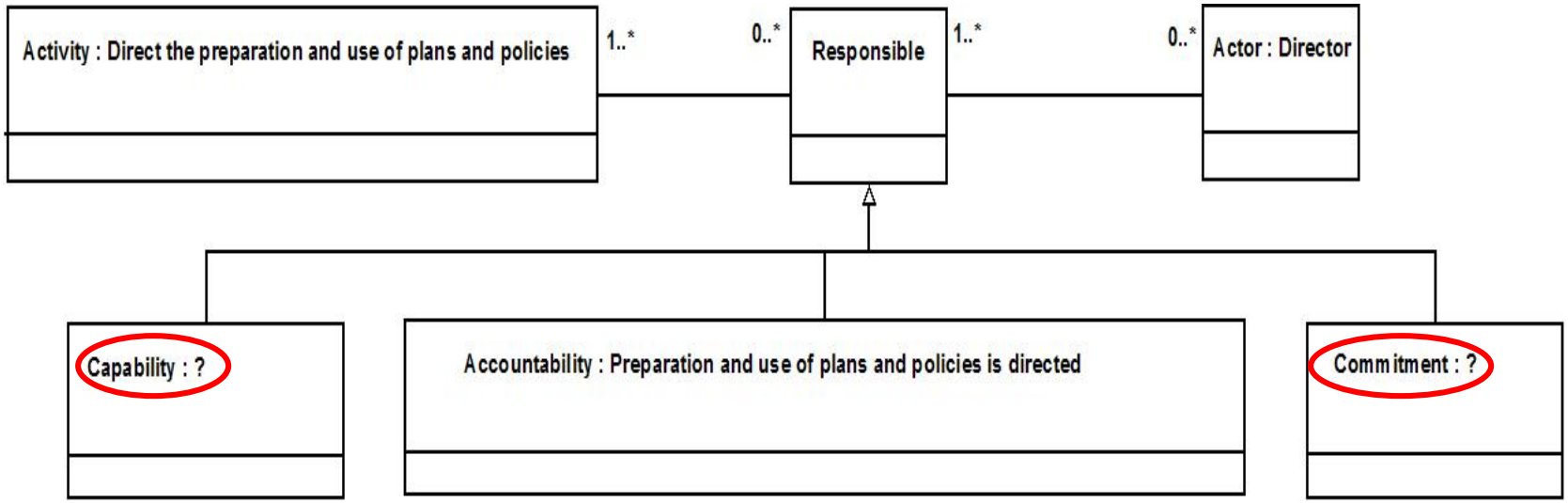
→ **Agent : Director**
→ **Activity : Direct the preparation and use of plans and policies**
→ **Accountability : Plans and policies**

The standard provides principles and not guideline
Is it improvable regarding the definition of responsibility ?

ISO/IEC 38500:2008

ISO/IEC 38500:2008

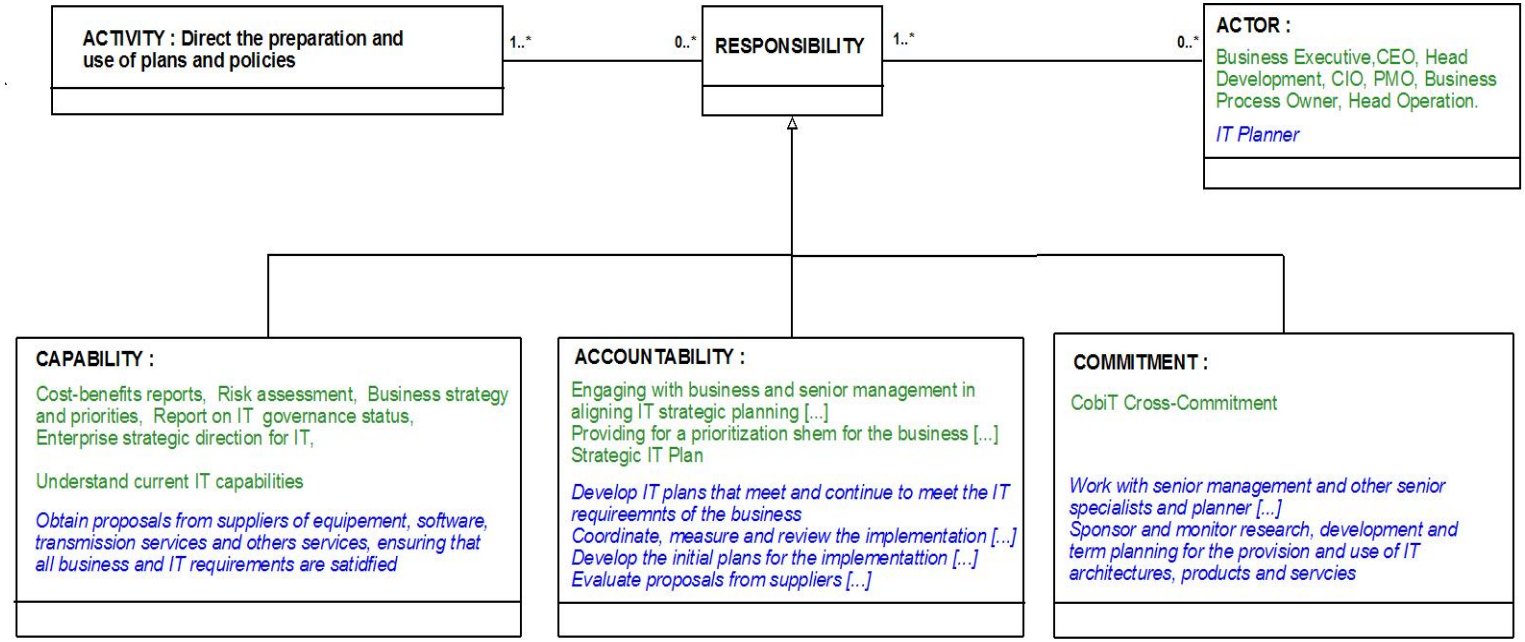
Director should direct the preparation and use of plans and policies that ensure the organization does benefit from the developments of IT



ISO/IEC 38500:2008

ISO/IEC 38500:2008

From principle to guide lines :



Information from :

CobiT : PO1 Plan and Organise : Define a Strategic IT Plan

ITIL : IT Planner role's objectives

Conclusions

ISO/IEC 38500:2008

→ 6 principles :

Principle 1 : Responsibility clearly defined and assigned

Responsibility may be model using Capability, Accountability and Commitment

1st illustration :

Creation of policies (business to IT) from business goals / processes and mapping with the standard ISO/IEC 15504

2nd illustration :

Enhancement of existing models; enhancement of CIMOSA to improve responsibility definition and assignation through enterprise architectures

3rd illustration :

Enhancement of the responsibility definition in governance principle and contribution to the translation of principles in guide-lines.

Thank you for your attention,
Question ?

REFERENCES

- Abou El Kalam, A., El Baida, R., Balbiani, P., Benferhat, S., Cuppens, F., Deswarte, Y., Miège, A., Saurel, C., Trouessin, G. (2003), Organization-Based Access Control, IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy'03), 4-6 juin 2003, Côme, Italie, pp 120-131.
- Antón, A. (1996), *Goal-Based Requirements Analysis*. Second ICRE'96, Colorado Springs, USA.
- Aubert, J., Gateau, B., Incoul, C., Feltus, C. (2008), *SIM : An Innovative Business-Oriented Approach for a Distributed Access Management*, International Conference on Information & Communication Technologies: from Theory to Applications (IEEE ICTTA2008), Damascus, Syria.
- Basel II (2006), Bank for International Settlements BIS: International Convergence of Capital Measurement and Capital Standards: Revised Framework – Comprehensive Version.
- Bertino, E., Mileo, A., and Provetti, A. 2005. *PDL with Preferences*. IEEE international Workshop on Policies For Distributed Systems and Networks, Policy 2005 – Vol. 00, IEEE Computer Society, Washington, DC, 213-222.
- CEN/ENV 12204 (1996): Advanced manufacturing technology – Systems architecture - Constructs for enterprise modelling, CEN TC 310/WG1.
- CobiT 4.1, *Control Objectives for Information and Related Technology*, Information Systems Audit and Control Association, http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981
- Crook, R., Ince, D., Nuseibeh, B., (2002) *Towards an Analytical Role Modelling Framework for Security Requirements*, Security Requirements Group, Departement of Computing, The Open University, Walton Hall, Milton Keynes, MK7 6AA, UK.
- Directive 95/46/EC (1995), European Union: Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Communities, pp. 28-31.
- Feltus, C. and Rifaut, A. (2007), *An Ontology for Requirements Analysis of Managers' Policies in Financial Institutions*, I-ESA2007, Madeira, Portugal.
- Feltus, C. (2008), *Preliminary Literature Review of Policy Engineering Methods - Toward Responsibility Concept*, ICTTA2008, Damascus, Syria.
- Ferraiolo, D. F., Sandhu, R., Gavrila, S., D. Kuhn, R., Chandramouli, R. (2001), Proposed NIST Standard for Role-Based Access Control, *ACM Transactions on Information and System Security*, 4 (3), 224-274.
- Gateau, B., Feltus, C., Aubert J., Incoul, C. (2008), *An Agent-based Framework for Identity Management: The Unsuspected Relation with ISO/IEC 15504*, RCIS 2008, Morocco.
- ISO/IEC 38500 (2008), International Standard for Corporate Governance of IT (IT Governance)
- ISO 9000:2005 (2005), Quality management systems - Fundamentals and vocabulary.
- ISO/IEC 15504-1 (2004): Information technology - Process assessment - Part 1: Concepts and vocabulary.
- ISO/IEC 15504-2 (2003): Information technology - Process assessment - Part 2: Performing an assessment.
- ISO/IEC 15504-5 (2006): Information technology - Software Process Assessment - Part 5: An exemplar process assessment model.
- ITIL (2001), *IT Infrastructure Library – Service Delivery*, The Stationery Office Edition, ISBN 011 3308930.
- Kosanke, K., Vernadat, F.B. and Zelm, M. (1999) *CIMOSA: enterprise engineering and integration Computers in Industry*, Volume 40, Issues 2-3, Pages 83-97.
- March, J. G. and Olsen, J. P. (1995) *Democratic Governance*, New York, The Free Press, 1995, 292 pp.
- Mauchan, M. (2007), thèse « *Modélisation pour la simulation de chaines de production de valeur en entreprise industrielle comme outil d'aide à la décision en phase de conception / Industrialisation* »
- Park, J., Sandhu, R., (2002) Originator Control in Usage Control, *Policy 2002*, Monterey, California, U.S.A.
- Rifaut, A. and Feltus, C. (2006), *Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach*, REMO2V'2006, Luxembourg
- Sarbanes, P. S. and Oxley, M. (2002) "*Sarbanes-Oxley Act of 2002*".
- Savén, R. S. (2002), *Process modelling for enterprise integration: review and framework*, 13th International Working Seminar on Production Economics, Igls/Innsbruck, Austria, February 18-22.
- Togaf (2007), *The Open Group Architecture Framework* (TOGAF 8.1.1 'The Book'), 2007 Edition , Van Haren Publishing
- Vernadat F. B. (1995), *Enterprise Modelling and Integration*, Chapman & Hall, London , ISBN 0-412-60550-3
- Vernadat, F.B. (2004), *Enterprise Modelling: Objectives, constructs & ontologies*, Tutorail EMOI-CaiSE Workshop, Latvia.
- Yu, E. S. and Liu, L. (2001). *Modelling Trust for System Design Using the i* Strategic Actors Framework*. Workshop on Deception, Fraud, and Trust in Agent Societies Held During the Autonomous, Eds. Lecture Notes In Computer Science, vol. 2246. Springer-Verlag, London, 175-194